ASSURMER AP n°8

Présentation des protocoles de sécurité Wi-Fi

Date version	Auteur	Validateur	Destinataires	Diffusion document	Nbr. de pages	Commentaires
07/01/25	Maxence MARTIN-PARENT + Antoine Rodrigues	Aucun	Service DSI	Interne via Teams	7	Document intégral

TABLE DES MATIERES

Introduction

La sécurité des réseaux Wi-Fi est une composante essentielle de toute infrastructure informatique moderne. Les protocoles de sécurité Wi-Fi ont évolué au fil du temps pour répondre à des besoins croissants de protection contre les cyberattaques. Cette étude comparative présente les différents protocoles disponibles, leurs caractéristiques, avantages, limitations et les recommandations d’utilisation.

Les différents protocoles

WEP (Wired Equivalent Privacy)

WEP, introduit en 1997 avec la norme 802.11 originale, a été le premier protocole conçu pour sécuriser les communications Wi-Fi. Ce protocole utilise l'algorithme RC4 pour le chiffrement des données, avec des clés de 40 ou 104 bits, auxquelles s'ajoute un vecteur d'initialisation de 24 bits pour atteindre une longueur totale de 128 bits. L'authentification peut être réalisée soit en mode ouvert (Open System Authentication), soit en mode partagé (Shared Key Authentication).

Malgré sa simplicité de configuration, WEP présente des failles majeures, en particulier dans la génération des clés, où les vecteurs d'initialisation sont souvent répétitifs. Cela le rend extrêmement vulnérable aux attaques, permettant aux pirates de le compromettre rapidement à l'aide d'outils tels qu'Aircrack-ng. Obsolète depuis 2004, WEP est aujourd'hui déconseillé, sauf en cas de contrainte matérielle ne permettant pas l'utilisation d'un protocole plus récent.

WPA (Wi-Fi Protected Access)

Introduit en 2003 comme une solution temporaire pour remplacer WEP, WPA utilise également l'algorithme RC4, mais avec le protocole TKIP (Temporal Key Integrity Protocol) pour renforcer la sécurité. L'authentification est disponible sous deux formes : WPA-PSK (Pre-Shared Key), destiné aux réseaux domestiques, et WPA-Enterprise, qui repose sur un serveur RADIUS pour les environnements professionnels.

WPA a corrigé certaines failles de WEP, notamment en introduisant un mécanisme de génération dynamique des clés pour chaque paquet. Toutefois, il hérite des limites de l'algorithme RC4, considéré comme non sécurisé, et de nouvelles vulnérabilités ont été découvertes dans TKIP, comme l'attaque Beck-Tews. Depuis l'introduction de WPA2 en 2004, WPA est désormais considéré comme obsolète.

WPA2 (Wi-Fi Protected Access 2)

WPA2, introduit en 2004 avec la norme 802.11i, marque une avancée significative dans la sécurité des réseaux Wi-Fi. Ce protocole remplace RC4 par l'algorithme AES (Advanced Encryption Standard) et utilise le protocole CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) pour un chiffrement robuste. Il offre deux modes d'authentification : WPA2-PSK pour les environnements domestiques et WPA2-Enterprise avec un serveur RADIUS pour les entreprises.

Pendant plus d'une décennie, WPA2 a été considéré comme le standard de sécurité des réseaux Wi-Fi. Cependant, des vulnérabilités comme l'attaque KRACK (Key Reinstallation Attacks) ont mis en évidence des failles dans le protocole de handshake. Bien que des correctifs logiciels aient permis de pallier ces faiblesses, WPA2 nécessite un matériel compatible AES pour fonctionner pleinement. Il reste néanmoins une option acceptable lorsque WPA3 n'est pas disponible.

WPA3 (Wi-Fi Protected Access 3)

WPA3, introduit en 2018, représente l'évolution la plus récente des protocoles de sécurité Wi-Fi. Il utilise l'algorithme AES-GCMP (Galois/Counter Mode Protocol) et introduit des améliorations significatives. En remplacement du mécanisme PSK (Pre-Shared Key), WPA3-Personal adopte le protocole SAE (Simultaneous Authentication of Equals), qui renforce la sécurité contre les attaques de dictionnaire hors ligne. Pour les environnements professionnels, WPA3-Enterprise propose un chiffrement renforcé avec des clés de 192 bits.

WPA3 améliore également la sécurité des réseaux publics grâce à OWE (Opportunistic Wireless Encryption), qui chiffre les communications même en l'absence d'authentification utilisateur. Bien qu'il nécessite des équipements modernes et que son adoption reste limitée en 2025, WPA3 offre un niveau de sécurité sans précédent et garantit une rétrocompatibilité avec WPA2 dans le cadre du mode de transition WPA3-Transition Mode.

OWE (Opportunistic Wireless Encryption)

Introduit avec WPA3 pour répondre aux besoins des réseaux ouverts, OWE propose un chiffrement des données sans nécessiter d'authentification utilisateur. Contrairement aux réseaux ouverts classiques où les données circulent en clair, OWE empêche l'interception passive des communications par des tiers.

Ce protocole est particulièrement adapté aux environnements où l'authentification utilisateur n'est pas pratique, tels que les cafés ou les bibliothèques. Simple à déployer, OWE offre une sécurité renforcée pour les réseaux publics. Cependant, il ne fournit pas de contrôle d'accès, car aucun mot de passe n'est requis, et nécessite des appareils compatibles pour fonctionner correctement.

Recommandations générales

Pour garantir la sécurité des réseaux Wi-Fi, il est essentiel de privilégier WPA3 chaque fois que cela est possible, notamment dans les environnements modernes. Si WPA3 n’est pas disponible, WPA2 constitue une alternative acceptable, à condition que les appareils soient à jour pour éviter les vulnérabilités comme KRACK. Les protocoles WEP et WPA doivent être évités, sauf dans des cas exceptionnels où les contraintes matérielles empêchent leur remplacement.

Pour les réseaux publics, l’utilisation d’OWE est recommandée, ou à défaut, la configuration de portails captifs avec WPA3 pour offrir un contrôle d’accès minimal. Dans les environnements professionnels, WPA3-Enterprise associé à un serveur RADIUS représente la solution optimale pour une sécurité accrue.

Conclusion

L’évolution des protocoles de sécurité Wi-Fi reflète la nécessité de s’adapter aux menaces croissantes dans un monde de plus en plus connecté. Dans un contexte où la confidentialité des données et la protection contre les intrusions sont prioritaires, le choix d’un protocole adapté est crucial. WPA3 se distingue aujourd’hui comme la solution la plus fiable et performante pour répondre aux exigences de sécurité des réseaux modernes.